

UK's new Research Institute investigates the science of cybersecurity

Government Communications Headquarters (GCHQ)



How do we know when we are “secure enough”? How do we decide how best to spend our precious security budget? How do we reduce our reliance on individual expert judgement and make better, more objective security decisions? It is always challenging to bring scientific rigor to bear on a complex, real world problem, and this challenge applies in spades to the relatively young discipline of cybersecurity. Practitioners must work hard to stay on top of ever changing technologies and a rapidly evolving threat environment, and simply keeping abreast of “best practice” is challenging. Yet we must—if we want to ever get ahead of the curve—develop a more systematic, rigorous approach based on foundational scientific knowledge and understanding.

The UK government recently announced the formation of a virtual Research Institute to improve understanding of the science behind the growing cybersecurity threat. The Institute, which is funded by a £3.8 million grant (\$6.14 million US), is part of a cross-government commitment toward increasing the nation’s academic capability in all fields of cybersecurity.

Established by the Government Communications Headquarters (GCHQ), in partnership with the UK Research Councils (RCUK) and the Department for Business, Innovation and Skills (BIS), the Research Institute is a virtual organization involving seven universities. It will allow leading academics in the field of cybersecurity, including social scientists, mathematicians, and computer scientists from across the UK, to work together. It will also connect them with the collective expertise of industry security experts and international researchers in the field—with a particularly close relationship expected with the US. The Research Institute opened for business on October 1, 2012, and is funded for a period of three and a half years.

Universities were selected following a tough competitive process in which they had to devise new research programs to address one of two key challenges:

- ▶ How secure is my organization?
- ▶ How do we make better security decisions?

Addressing these very practical challenges requires a blended approach from researchers, drawing from both technological and behavioral disciplines. Four teams were successful:

- ▶ University College London, working with University of Aberdeen;
- ▶ Imperial College, working with Queen Mary College and Royal Holloway, University of London;
- ▶ Royal Holloway, University of London; and
- ▶ Newcastle University, working with Northumbria University.

University College London (UCL) was selected to host the Research Institute, with Professor Angela Sasse taking the role of director of research. At the press launch, Sasse acknowledged the strong multi-disciplinary nature of the research portfolio, saying, “I am delighted to be leading the new Research Institute. This is an opportunity to work closely with colleagues from different scientific disciplines to tackle the technical, social, and psychological challenges that effective cybersecurity presents.”

As well as being cross-disciplinary, the research portfolio is an exciting blend of theoretical work and experimentation in “the field”—with “the field” meaning real organizations, operational information technology (IT) systems, and real, live users. The work

is unusual in being focused firmly on improving security within organizations rather than for individual citizens. It is equally applicable to governmental or commercial organizations. The collaborative approach between academia, industry, and government will ensure that research is relevant and inspired by real world, cutting edge security issues.

The winning projects

UCL's project is entitled “Productive security: Improving security compliance and productivity through measurement” and will focus on the behavior of users within the workplace. This work builds on a growing body of evidence that security policies and control are not fully effective because employees either cannot or will not comply with them [1, 2]. A key reason for noncompliance is the combination of employee workload and the complexity of security controls chosen. Yet many security decision makers do not factor the impact on employees, their tasks, and the company's business processes into their decision about which security controls to put in place. Current attempts to educate employees about the need for security are of questionable effectiveness because they simply push more information on people who are already overworked. Even in organizations with high security awareness, noncompliance can be observed because the security policy causes excessive friction or is not agile enough to meet the needs of the business [3, 4].

The project will work with at least two major companies to collect data on employees' workload, risk perception, and the resulting security behaviors. It will use that data to develop a decision support model to allow security professionals to balance the impact of security controls on employees and business processes against the risk mitigation the controls can achieve.

The lead researchers are Professor Angela Sasse of UCL and Professor David Pym of University of Aberdeen.

In contrast to UCL, the three-party team led by Imperial College will work on the Research Institute's most heavily theoretical program. The project, “Games and abstraction: The science of cybersecurity,” will develop new approaches to decision support based on mathematical game theory. The project is academically ambitious in attempting to combine three major disciplines: game theory, machine learning, and abstract

interpretation. For example, no connection has been established so far between abstract interpretation and these other areas.

Game theory, the theory developed for the mathematical analysis of multiperson strategic decision making [6], has been increasingly applied in the last decade in cybersecurity. Examples of applications can be found in the fields of intrusion detection systems, anonymity and privacy, economics of network security, and cryptography. A state of the art survey of these applications is given in Alpacan and Basar's *Network Security: A Decision and Game Theoretic Approach* [7]. This new work will build on the game theoretical model developed by Lye and Wing [5]. A limitation of this work is that the attacker model is based on a set of known strategies; part of the proposed research is to extend the approach to deal with previously unseen attacks (e.g., zero days) and emerging behaviors. The research objectives are to:

- ▶ Model complex scenarios by developing mathematical abstraction techniques for stochastic games, using techniques originating in probabilistic abstract interpretation and machine learning;
- ▶ Provide a precise way to analyze how results of optimal behavior in the abstract models relate to the optimal or near-optimal behaviors in complex real scenarios; and
- ▶ Demonstrate the results by proof-of-concept implementations and test on realistic data provided through empirical studies.

The lead researchers are Professor Chris Hankin of Imperial College; Professor Dusko Pavlovic of Royal Holloway, University of London; and Dr. Pasquale Malacaria of Queen Mary College.

Royal Holloway, University of London's project



FIGURE 1. The University College London will host the Research Institute, a virtual organization that will bring together cybersecurity experts from around the world.

is entitled “Cybersecurity cartographies.” Its goal is to develop ways of visualizing the different means in which both people and technology protect important data. The project brings together the disciplines of art and design, network security, and organizational security in order to develop a range of visualization techniques that better inform security managers about the strength of data protection across their cyber estate.

Security managers use a combination of organizational, physical, and technical controls to provide robust information asset protection. Control lists, such as those in Annex A of ISO 27001 (i.e., an information security management system standard), have long acknowledged the need for the three types of control, but no methods are available to systematically combine them. In addition, risk management techniques do not include visualization methods that can present a combined picture. To address these gaps, the project will further develop existing research on the influence of cultural and organizational techniques on policy compliance [8]. It will also develop techniques to combine interpretive cartography with informational cartography using a visualization framework [9]. In addressing these gaps, the work will help security managers to develop well informed trade-offs between security and other business drivers, while supporting



FIGURE 2. The Research Institute's director of research is Professor Angela Sasse of University College London.

their existing skills and expertise.

The lead researcher is Dr. Lizzie Coles-Kemp of Royal Holloway, University of London.

Finally, Newcastle University is working on the project “Choice architecture for information security.” Newcastle’s research hypothesis is that there exists a rigorous choice architecture which will nudge decision makers to make demonstrably better information security decisions. Newcastle’s approach takes inspiration from the work on nudging from the behavioral economics community [10]. Nudging provides a framework to influence decision makers in a subtle way. The theory will be applied to scenarios relating to consumerization [11] (i.e., the use of personal devices in the workplace) and will also be relevant to the broader issue of work-life integration (i.e., the blurring of the boundaries between work and home life).

In addition, part of the novelty of the approach will be the ability to integrate rigorous security assessment

with psychological ownership models adapted from the occupational psychology literature [12, 13].


The research objectives are to:

- ▶ Understand the psychological phenomena that dictate security behavior relevant for data protection in consumerization scenarios, from the various perspectives of the chief information security officer, IT administrators, and employees;
- ▶ Develop a choice architecture for these scenarios;
- ▶ Implement a toolset to implement the choice architecture—steering the decision maker to “better” decisions; and
- ▶ Experimentally evaluate the improvements delivered.

The lead researchers are Dr. Aad van Moorsel of Newcastle University and Professor Pamela Briggs of Northumbria University.

Conclusion

In mid-2012, GCHQ, BIS, and RCUK awarded the Academic Center of Excellence (ACE) in Cybersecurity Research to eight UK universities [14]. This initiative, the first part of a broad, joint response to the UK government’s national cybersecurity strategy [15], will enhance the UK’s cyber knowledge through original research.

The establishment of the Research Institute is another part of the broad response to the UK government’s national cybersecurity strategy [15]. The strategy describes how the government is working with academia and industry to make the UK more resilient to cyberattacks. Both the ACE and the Research Institute initiatives are harnessing the vital role that academia has to play in supporting and developing the UK’s capability in cybersecurity. 

About GCHQ

Government Communications Headquarters (GCHQ) is one of three UK intelligence agencies. GCHQ provides intelligence, protects information, and informs relevant UK policy to keep our society safe and successful in the Internet age.

References

- [1] Sasse MA, Brostoff S, Weirich D. “Transforming the ‘weakest link’—a human-computer interaction approach to usable and effective security.” *BT Technology Journal*. 2001;19(3):122–131. DOI: 10.1023/A:1011902718709
- [2] Beautelement A, Sasse MA, Wonham M. “The compliance budget: Managing security behaviour in organizations.” In: *Proceedings of the 2008 New Security Paradigms Workshop*; Sep 2008; Lake Tahoe, CA; p. 47–58. DOI: 10.1145/1595676.1595684
- [3] Pallas F. “Information security inside organizations—a positive model and some normative arguments based on new institutional economics” [PhD thesis]. [Berlin (Germany)]: Technical University of Berlin; 2009.
- [4] Albrechtsen E, Hovden J. “The information security digital divide between information security managers and users.” *Computers and Security*. 2009;28(6):476–490. DOI: 10.1016/j.cose.2009.01.003
- [5] Lye KW, Wing J (2005). “Game strategies in network security.” *International Journal of Information Security*. 2005;4(1–2):71–86. DOI: 10.1007/s10207-004-0060-x
- [6] Neumann J, Morgenstern O. *Theory of Games and Economic Behavior*. Princeton (NJ): Princeton University Press; 1944. ISBN-13: 978-0-691-13061-3
- [7] Alpacan T, Basar T. *Network Security: A Decision and Game Theoretic Approach*. Cambridge (MA): Cambridge University Press; 2011. ISBN-13: 978-0-521-11932-0
- [8] Pieters W, Coles-Kemp L. “Reducing normative conflicts in information security.” In: *Proceedings of the 2011 New Security Paradigms Workshop*; Sep 2011, Marin County, CA; p. 11–24. DOI: 10.1145/2073276.2073279
- [9] Hall P. “Bubbles, lines and string: How information visualization shapes society.” In: Blauvelt A, Lupton E, editors. *Graphic Design Now in Production*. Minneapolis (MN): Walker Art Center; 2011. p. 170–185.
- [10] Sunstein C, Thaler R. *Nudge: Improving Decisions about Health, Wealth, and Happiness*. New Haven (CT): Yale University Press; 2008. ISBN-13: 978-0-300-12223-7
- [11] Microsoft Corporation (2011). “Strategies for embracing consumerization.” 2011. Available at: <http://download.microsoft.com/download/E/F/5/EF5F8B95-5E27-4CDB-860F-F982E5B714B0/Strategies%20for%20Embracing%20Consumerization.pdf>
- [12] Ifinedo P. “Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory.” *Computers and Security*. 2012;31(1):83–95. DOI: 10.1016/j.cose.2011.10.007
- [13] Aurigemma S, Panko R. “A composite framework for behavioral compliance with information security policies.” In: *Proceedings of the 45th Annual Hawaii International Conference on System Sciences*; Jan 2012, Maui, HI; p. 3248–3257. DOI: 10.1109/HICSS.2012.49
- [14] GCHQ. “UK universities awarded Academic Centre of Excellence status in Cyber Security Research” [Press release]. Available at: <http://www.gchq.gov.uk/Press/Pages/Cyber-Security-Research-Centres-of-Excellence.aspx>
- [15] UK government cabinet office. “The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world,” 25 Nov 2011. Available at: <http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf>